

特開平10-228727

(43)公開日 平成10年(1998)8月25日

(51)Int.C1.^a

G 11 B 20/10

識別記号

F I

G 11 B 20/10

H

審査請求 未請求 請求項の数1

OL

(全9頁)

(21)出願番号 特願平9-353867
 (22)出願日 平成9年(1997)12月22日
 (31)優先権主張番号 033543
 (32)優先日 1996年12月20日
 (33)優先権主張国 米国(US)

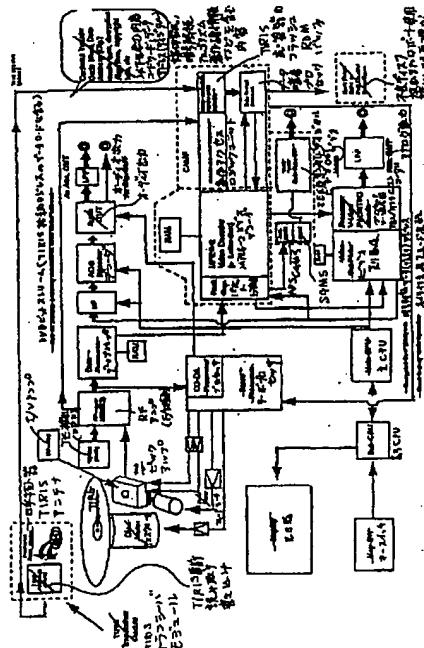
(71)出願人 590000879
 テキサス インスツルメンツ インコーポ
 レイテッド
 アメリカ合衆国テキサス州ダラス, ノース
 セントラルエクスプレスウェイ 13500
 (72)発明者 ピルバックス (マドフ) ネルリカル
 アメリカ合衆国テキサス州プラノ, キヤロ
 ル サークル
 (72)発明者 ロイ アイ. イーデンサン
 アメリカ合衆国テキサス州リチャードソン,
 アポロ コート 404
 (74)代理人 弁理士 浅村皓 (外3名)

(54)【発明の名称】著作権設定プログラム媒体を保護するためのTIRISに基づくBIOS

(57)【要約】

【課題】光媒体などの上にデジタル的に記録された著作権物の違法コピーを防止し、防犯以外の利益を著作権者など関連する人々に提供する方法を提案する。

【解決手段】"TIRIS"トランスポンダをDVDディスクの中心部に埋め込む。呼掛け器を内蔵した媒体再生装置にDVDが挿入されると呼掛けを行い、トランスポンダは暗号解読に必要な情報を応答する。この情報に基づいて再生装置はDVDの暗号を解読し復号して再生する。"TIRIS"トランスポンダは光学的にコピー出来ないので違法コピーへの耐性が強化採れると同時に、情報量も従来より多いため、在庫管理などにも使用できる。



【特許請求の範囲】

【請求項1】著作権設定物のみを任意のデジタル媒体システムの中で再生可能または使用可能とすることを保証するための方法であって、

呼掛信号をトランスポンダ（応答器）に送信して、それに応答するトランスポンダ応答信号を受信するための無線周波数インタロゲータ（呼掛け器）を、I/Oポートを有する媒体再生装置に統合するステップと、

トランスポンダを予め定められた媒体要素に取り付けるステップであって、前記媒体要素はデジタル媒体内容物ストリームを有し、また前記トランスポンダは暗号解読アルゴリズムを含むトランスポンダ応答信号を、前記呼掛け信号を受信したことに応答して送信する、前記ステップと、

トランスポンダ応答信号を受信し、前記暗号解読アルゴリズムをプロセッサに提供するステップと、

前記デジタル媒体の内容物ストリームを処理するために、前記暗号解読アルゴリズムに基づいて前記プロセッサを構成するステップと、

を含む前記方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は一般的に防犯目的でのRF-IDシステムの使用に係わり、更に詳細には著作権設定物の知的財産価値の保護に関する。

【0002】

【従来の技術】RF-IDシステムはより多くのそして広範なアプリケーションで益々使用されるようになってきている。典型的なRF-IDシステムに於いて、インタロゲータ（呼掛け器）は、呼掛け信号をトランスポンダ（応答器）にその呼掛け器の読み取り範囲内で送信し、そしてトランスポンダは、呼掛け信号を散乱をさせて返信することによりその識別番号を完全二重モードで送信するか、またはトランスポンダが呼掛け信号によって起動された後に実際にその識別信号を半二重モードで送信することにより応答している。RF-ID技術は防犯マーケットに適所を見い出した。トランスポンダは防犯バッジ、料金札、またはゲート通行証に簡単に取り付けられて、アクセスの許可／禁止を行ったり自動請求サービス、すなわち有料道路および駐車場など、を実施することも出来るし、また読みとり器は料金所および出入り口通路に簡単に取り付けることが出来る。更に小規模であっても、RF-IDシステムは広範な種々の商品に対して防犯と追跡機能とを提供することが出来る。卸売り倉庫、図書館、および製造プラントは全て、RF-IDシステムの追跡機能に関して使用する可能性のある現場である。しかしながらRF-IDシステムの防犯機能に関しては、秘密または重要機密政府文書の追跡と防犯が物理的物体、すなわち文書へのアクセスを許可するかまたは禁止するかに注目した領域の1つである。更に物体

10

20

30

40

50

の追跡および防犯からの拡張として、オリジナルの著作権設定物、すなわちオリジナルのデジタルビデオディスク（DVD）並びにデジタルビデオカセット（DV）のみがプレーヤ、すなわちDVDプレーヤ上で再生出来るようにすることがあげられる。

【0003】著作権／反テープに関する保護を実施するために現在利用可能な方法のほとんどは、”警告ラベル”に毛の生えた程度の防止効果である。このプログラム媒体はほとんどがアナログの、“ブランド物”マルチメディアの内容であり、例えば有名スタジオ映画の録画済VHSテープ、CD、カセット、ケーブル／衛星チャンネルで放映された映画等々である。録音した音楽家、有名スタジオおよび同様の人々はこの様な不完全な保護手段で我慢してきたが、それは最近まで複写物の品質が、オリジナルマスター媒体自体の品質までは複写出来ないので十分に劣化させられていたからである。実際1つの政令が存在しており、1992年のHRA法では著作権物のアナログコピーを1度に1つ行って再生することが許されている（すなわち、もしもあなたがカセットを車の中に忘れるとなれば使用できなくなる場合に、法令はあなたの自身が使用するために別のコピーをとることを許しているが、しかしながら販売するために多数のコピーをとることは認めていない。）

【0004】今日市場に於いて取り外し可能なデジタル媒体の急速な発達により、この様な装置を広い範囲の種々の発表目的のために保存して使用することが便利になってきている。特に光ディスク媒体は大量のデジタルデータおよび情報を発表する比較的低価格の方法を提供する。この“発表された”または編集された情報の性質は、娯楽映画からゲーム、会話型トレーニング、X線またはその他の画像ファイルまで非常に広い範囲に変化する可能性がある。光ディスク媒体のコピーは著作権侵害に対抗して保護するのが最も困難な形式の媒体であり、それはオリジナルディスクを光学的にコピーすると保護体系もまた後に続く偽造媒体にコピーされてしまうからである。これに加えて、もしもその保護体系がデジタル的である場合、ハッカーは保護手順を迂回して保護を破ることができるのはずである。アナログコピーとは異なり、“完全”デジタルコピーの本質的な性質上、複写物はオリジナルと別物とすることが出来ない。更に、これらのコピーを許可されていない方法で再配布または再構成されることにより、売り上げの損失および所有者の真正の財産の法的権利が不当表示されてしまう恐れがある。

【0005】光ディスク偽造問題に対する1つの解決策として、1996年5月2日に申請されテキサスインスツルメント社に委譲された出願番号60/016,745号の係属中の出願には、TIRIS暗号が導入されており、ここではTIRISトランスポンダが媒体の中に組み込まれていて、媒体を媒体再生装置に挿入した時点

で媒体再生装置がトランスポンダに呼掛けを行い、トランスポンダは媒体自体の上に配置されているデータワードのアドレスと、コードワードとを応答する。媒体再生装置は次にそのデータワードを媒体上の特定のアドレスに配置し、もしも受信されたデータワードと読み取られたデータワードとが一致すると、その媒体再生装置はその媒体を再生する。T R I S 暗号は偽造ディスクの製造を思いとどまらせるだけの力を有するが、それはT R I S トランスポンダは光学的にコピーすることが出来ず、また暗号コードデータを簡単にはハック出来ないからである、これは特にトランスポンダとトランシーバとの間にRFリンクを使用することにより、知られ得ない技術を採用できるためである。このコードデータは、もしも完全な集積構築技法を用いて配備されたとすると、ホストマシンのデータバス上に出現することを防止できるので、外部からのアクセス、ハッキングそして/または改悪から完全に絶縁される。この解決策に関して生じる問題は経済的負担のほとんどの部分が、著作権媒体の上に何らかの機能を実行する再生装置および周辺機器に掛かり、最大の利益が著作権保有者、すなわち米国映画協会にもたらされる点である。例えば、仮にその媒体がデジタルビデオディスクであったとすると、著作権保有者のコスト増加は、媒体自体へトランスポンダを追加するだけで、おそらく1ドル程度である。一方、周辺装置製造者はそのDVD再生装置に呼掛け器を追加する必要があり、また恐らくはディスク上の特定アドレスを読み取ることの可能な追加回路も必要であって、標準DVD再生装置で増加コストは数百ドルに達するであろう。ここに問題がある。

【0006】

【発明が解決しようとする課題】この様な発表方法が、著作権が設定されてたりまたは機密を必要とするソースデータに採用される場合、その様なデータの管理と配布とを保証する何らかの改善された方法は、その媒体のデータトラック上に含まれる実際のデータとは独立に採用される必要がある。更に、著作権物の使用を保証する方法はソフトウェアおよびハードウェアハッキングのいずれに対しても強固でありかつ耐性を有するものでなければならぬ。侵害は、保護システムを役に立たなくし、また正当な所有者を著作権法違反または同様な被害に曝してしまう。従って、全体として効果的なシステムとして、偽造保護の特質およびコピー防止機能を提供しなければならない。

【0007】

【課題を解決するための手段】以下に説明する保護システムは、在庫管理、使用に応じて価格決めがなされる取引、階層レベルでのアクセス制御および人口統計データ収集を含む、価値が関連し合うすべての利害関係人に対して、更に別の潜在的な利益を提供する。T R I S 暗号（テキサスインスツルメント社の登録ならびに認証シ

ステム）手法のユニークな性質は、新たなレベルの複雑さでパッケージ化された媒体部材の管理ならびに追跡を可能とし、著作権所有者に更なる価値と保護とをもたらすことが出来るようにしている。T R I S 暗号器は平らで電池が不要な無線周波数半導体トランスポンダパッケージであって、これは著作権が設定されたDVD媒体の中心部に接着されているかまたは埋め込まれている。再生装置内に配置されたT R I S トランシーバでのみ読み取ることの可能な種々の符号化そして/またはスクランブルされた情報ビットで暗号化されることで、ディスクは許可チェックがなされる。

【0008】本発明はハードディスクドライブ構造を含み、これはトランスポンダからハードディスクドライブの中にダウンロードされる情報レベルを含む。将来の周辺機器はどの形式の媒体が周辺機器の中に挿入されたかを識別できるようになるであろう。例えばDVDディスクをDVD再生装置に挿入した際に、この再生装置はたとえこの再生装置を運転する前であっても、媒体装置上に配置されているトランスポンダを読み取り、この読み取り結果でBIOSに対して、DVDディスクを再生するのに必要な動作設定を提供するはずである。BIOSが従来の様にハードディスク上に配置されていたりまたはこの例の様に再生装置の中に配置されているところで、BIOSを媒体素子の上に配置することにより、媒体を偽造再生に対して保護する責任が著作権所有者に移される。BIOSに関して、著作権所有者は例えば、実行されるべき媒体の型式、もしも許されている場合はコピー数、どの時点でその媒体が動作可能となるか、すなわち地域別公開の取り扱いの様な多くの運転パラメータを定義するはずである。更に詳細には、1つまたは複数の暗号解読キーそして/または種々のアルゴリズムをトランスポンダ自体の上に存在させることで、DVD再生装置またはドライブがその様な暗号解読アルゴリズム（またはそのポインタ）をその内蔵フラッシュROMの中にロードすることが可能となり、内蔵されている条件付きアクセス管理処理装置（C. A. M. P. ）が個々の内容に依存した暗号解読そして/またはスクランブル解除、復号などをディスク毎に実行できるようになる。

【0009】

【発明の実施の形態】T R I S の様な埋め込み型トランスポンダ（平板で円形形式、直径約1インチ（2.54センチ）、厚さおよそ0.5ミリ）を種々のデジタル式記憶媒体に対して媒体製造工程で組み込むことが可能である。単ページ基線トランスポンダは256ビットから512ビットのメモリを有するようになる。これらのビットはユニークなID/シリアル番号、コードワード、媒体型式、暗号解読アルゴリズム、著作権情報、そして媒体自身内部の”符号化または暗号化”アドレス位置等を記憶するように配置されている。このディスクアドレスは特定データワードのポインタとして機能し、

これはディスクのプログラム部材内の何処にでも埋め込まれる。ディスク上でデジタルデータストリーム（認証が確認されるまでプログラム内容を見る人にはアクセス不能）内に含まれるこのユニークなデータワードが次に、トランスポンダ自体のメモリ内に配置されている予め割り当てられたコードワードと比較される。コードワードとその他のトランスポンダ応答信号の暗号解読ならびにDVDビットストリーム（予め定められたアドレスに格納されたデータワードを含む）の連続的な暗号解読が実施され、そして媒体データワードとコードワードとが一致すると、認証が完了し内容を再生するためにアクセス出来るようになる。

【0010】しかしながら、もしもそのデータワードとコードワードとが一致しないか及び／またはトランスポンダから送信されたアルゴリズムでDVDビットストリームの暗号解読に失敗して、例えば復号することが出来ない場合は、いくつかの方法が取られる。最も簡単なのは、DVDを再生しないことである。再生出来ないディスクを放出するための信号を送るか、または出力ポートを非動作状態にするかまたはそうでなければ構成変更するようにビデオポートを再構成する。

【0011】本発明をここに更に詳細に説明する。トランスポンダからハードディスクドライブへダウンロードされる情報レベルを含むハードディスクドライブ構成方法が開示されている。将来の周辺装置はその周辺装置にどの形式の媒体が挿入されたかを識別出来るはずである。例えば、DVDディスクをDVD再生装置の中に挿入した時点で、その再生装置は再生装置が動作可能となる前であっても媒体装置上に配置されたトランスポンダを読み取り、この読み取り結果でBIOSに対して、DVDディスクを再生するのに必要な動作設定を提供するはずである。BIOSが従来の様にハードディスク上に配置されていたりまたはこの例の様に再生装置の中に配置されているところで、BIOSを媒体素子の上に配置することにより、媒体を偽造再生に対して保護する責任が著作権所有者に移される。BIOSに関して、著作権所有者は例えば、実行されるべき媒体の型式、もしも許されている場合はコピー数、どの時点でその媒体が動作なるか、すなわち地域別公開の取り扱いの様な多くの運転パラメータを定義するはずである。更に詳細には、暗号解読キーをトランスポンダ自体の上に存在させることで、DVD再生装置またはドライブがその様な暗号解読アルゴリズム（またはそのポインタ）をその内蔵フラッシュROMの中にロードすることが可能となり、内蔵の条件付きアクセス管理処理装置（C.A.M.P.）が個々の内容に依存した暗号解読そして／またはスクランブル解除、復号などをディスク毎に実行できるようになる。これによって、媒体内容の暗号化が複雑であることまたは少な過ぎること、すなわち0から32ビットの責任が著作権所有者に戻され、彼らが媒体が製造される際

に暗号化の詳細を定義する。従って希望する量の保安を各著作権所有者が個人的に定義出来る。

【0012】CAMPは少なくとも以下の要素を含む、図1および図2に図示されるように、条件付きアクセス論理ユニットおよびTIRISトランスポンダFLASHROMバッファである。条件付きアクセス論理ユニットがCAMPの中に見られるが、これはDVDビットストリームを受信するためのものであって、このビットストリームはあらかじめ定められた何処かのアドレスに配置されたTIRISデータワードとディスク読み取り機からのDVDの全てのデジタル内容を含む。ディスクの読み取りを開始する前であっても、ディスク読み取り機内の呼掛け器はディスク上に配置されているトランスポンダに呼び掛けを行ない、トランスポンダは呼掛け器に対してコードワード、データワードのアドレス、媒体型式情報、暗号解読アルゴリズムおよび著作権情報を含むデータストリーム、または言葉を変えればBIOSまたは条件付きアクセス管理処理装置（CAMP）用の設定情報を返信する。CAMP内でトランスポンダ応答データストリームはFLASHROMバッファの中に格納され、これはデータ暗号解読処理装置に格納済みデータを供給し、再生装置がデジタル媒体の処理（暗号解読、スクランブル解除および復号）をする準備を行う。

【0013】この再生装置の準備には種々の作業が含まれており、デジタル媒体を適切に復号するためのMPEG-2デコーダのセットアップ、不良ディスクを放出するようにポートを構成するかまたは再生を禁止するよう既存のポートを再構成することが含まれ、そしてもしもその媒体がかなり過去の種類（TIRISをディスクに実装する以前のもの）である場合は、条件付きで過去の動作モードで再生を許可する。MPEG-2デコーダのセットアップと言えどもいくつかのステップを取るが、それはどの型式の媒体が表示されるかに依存してMPEG-2プロセッサを異なるようにセットアップしなければならないからである。例えば、もしもその媒体要素がデジタルビデオディスク（DVD）の場合は、MPEG-2デコーダはデジタル音楽ディスクをデコードする場合に比べてかなり異なるようにセットアップされなければならない。更に、暗号解読アルゴリズムはその媒体のデジタル内容を解読するために使用されるアルゴリズムを定義し、媒体型式情報はプロセッサに対して再生される媒体の型式によって全く異なるセットアップパラメータを提供し、また著作権情報は例えば再生が許される回数を提供する。トランスポンダ応答データストリームがデータ暗号解読プロセッサに入力されると、全DVDビットストリーム（埋め込みデータワードを含む）に加えて全トランスポンダ応答データストリームのスクランブルの解除または暗号解読がビットストリームの復号を行なう前に実施される。FLASHROMは選択的なバッファメモリであって、FLASHROM

の能力によって大容量のデータを一度に消去したりプログラムすることが出来る。従って、ドライブ／サーボデジタル信号プロセッサ（D S P）の一部は内容物提供者（すなわちMGM）から復号に先だって暗号解読またはスクランブル解除を実行するために指示される処理（すなわち、動画エキスパートグループ（M P E G）－2）を事前に定める種類の“容器”として機能する。

【0014】これに代わって、違法コピーされたディスクはT I R I S無しでも識別できるであろうから、M P E Gデータストリームのスクランブルを解除するために暗号解読アルゴリズムは利用されないはずである。加えて、周辺装置内の命令は要求される過去の版（T I R I S暗号以前）との一致またはT I R I S認証試験に失敗するとディスクを強制的に放出するように出来る。また、出力ポート不能化そしてまたはインターフェース再構成を偽造媒体、または使用時間切れ媒体または配布の管理または制限（時間または用途ベースで）が必要な媒体を検出した時点で採用することも可能である。

【0015】正当に記録されたが暗号化されていないディスクについてはM P E Gデータストリームを再生できなければならぬであろうが、しかしながらドライブ内に組み込まれたM P E Gデコーダのハードウェアを通してではなく、もしも可能であれば何処か別の場所でM P E Gソフトウェアデコーディングを通して、すなわちホストマシンマイクロプロセッサの中で行われるべきである。このことは、ハードディスクドライブ（H D D）製造者が、米国動画協会（M P A A）の承認を受けた媒体（媒体のトランスポンダ内に埋め込まれた暗号解読データでコピー防止がなされている）を再生するために、T I R I Sに準拠した構成のハードウェアを彼らのドライブ設計の中に組み込むことを勇気づけるであろう。しかしながら、ソフトウェアデコーディングに依存して、暗号解読コードが何処かのソフトウェアに搭載されている場合を除いてはそれ以上の暗号化処理を行なえない、より安価なドライブを製造することも可能としている。

【0016】意図しているトランスポンダ応答データストリームのビット割り当て計画の例を以下に説明する。この例の中でトランスポンダ応答データストリームの最初の3 2 ビットの用途には製品追跡データが含まれております、これは著作権設定物の製造ならびに在庫管理に関する詳細な記録情報が含まれている点を注意しておきたい。示されているいくつかの例は、製造S K U 、バッチ番号、日時および番地である。データの中央の1 6 0 ビットは、D V D自身の上のデータワードの6 4 ビット物理アドレスを含み、次の6 4 ビットはT I R I Sトランスポンダコードワードに割り当てられている。後部の3 2 ビットは3 2 ビットアルゴリズムを含み、トランスポンダデータストリーム全体と、同様にD V Dビットストリーム全体とを暗号化するために使用される。この例に関して続けると、最後の6 4 ビットを製造後書き換え

10

20

30

40

50

可能データを含むようにとっておくことが可能であり、例えば運転／経過の表示や、媒体が再生または使用された回数を計数する回数カウンタを含み、すなわち視聴時間毎支払いや、運転固有価格付けのために許可された運転回数を制限したり、また“書き込み”サイクルの回数を記憶するためのものである。更に進んだ読者は、これらのビットを使用して遠隔制御ポーリング機能を実現することが出来るであろうが、これは媒体使用状況の追跡が切符販売状況（after ticket sales）と同様に例えばニールセンのような放送のみに基づく視聴率調査機構から離れるにつれて生じるであろう。更にこのシステムで生成される、実時間使用データ、取扱量監査傾向からのトレンドは、使用者がリアルタイムのニールセンの様な（視聴率追跡）評価を著作権所有者、内容物所有者、小売り人のO E M等にフィードバックすることを可能とする。T I R I Sシステムを具備した再生装置はリアルタイムでポーリングされることが可能であり（ネットワークカードの双方向通信を通して）、対象聴取者に適切な広告を提供することが出来る。これは広告主が製品商標の浸透、推進等を計る際に非常な利点となる。

【0017】D V Dまたは媒体再生装置所有者に対する別の機能は、T I R I Sトランスポンダ情報を媒体に基づく情報と共に使用して個人媒体内容ライプラリ管理機能を生成することである。

【0018】防犯手法の完全性を更に保護するために、T I R I S読み取り器／呼掛け器の機能ならびに一致確認処理手順が内部的に完結されなければならない、すなわち呼び掛け器I Cの内部通信バス上で完結されなければならない。動画エキスパートグループ（M P E G）デコーダをまた同様に媒体再生装置の知的機能の中に配置して、コード破りおよび保護を打ち破ろうとする試みを非常に困難なものとすることが出来る（取り扱う‘平文’のデジタルビットが存在しない）。T I R I S呼掛け器／読み取り機およびM P E Gデコーダを单一I Cチップ上に統合することは非常に望ましく、それはその様な構造が著作権保護の保証を助けるからである。

【0019】許可確認に成功した時点で、使用方法およびその他の使用者ビット計数器、ならびにトランスポンダの書き込み可能要素が、価値連鎖、例えば小売り人、貸出し人、再販人、最終使用者および内容提供者またはその代理人、すなわち知的財産権／使用料を集金するサークルパーティーまたは代理店等の中でアクセス可能となる。“ブランド付き”内容物が本物と確認できない場合は、D V Dは“無許可プログラムコピー”を検出したことを表示することが出来る。T I R I S読み取り機は次に事前に記録されていた、恐らくはスクリーン表示器（O S D）メッセージとして格納されているはずの著作権警告／注意の位置に切り替える。

【0020】高度な目的のアプリケーション、すなわち読み取り／書き込みを使用した、多重ページトランスポ

ンダ、在庫管理、後方業務ならびに小売り管理機能が可能であり、小売人、装置製造者（ハードウェア〇ＥＭ）、再販人および再分配人にもまた利益が実現される。製造日時／場所、版／カタログ番号の様な”予め入力されるオリジナルデータ”をDVDの中に埋め込んで暗号化して、既に取得済みの正当な媒体のための優れた過去のシステムを使いつぶすことが可能となる。新たに出現するDVD再生装置は種々の媒体型式を区別できるものと期待される。

【0021】もしも媒体が以前の型式（音楽CDまたはCD-ROM等の様に）と判定されると、DVD再生装置/TIRISはもちろんMPEGデータストリームを復号する必要はなく、従ってその様な媒体を過去の動作モードで正常に再生することを可能とする。過去の動作モードに於いて、図1および図2に示すように、一度CAMPがその媒体を過去の型式の媒体であると認識すると、媒体の内容は復号されずに、サーボ／プロセッサにその媒体を再生させる命令が発せられる。一方、オリジナルの本物のTIRIS暗号が付けられていないDVD媒体の場合は（すなわち、TIRIS暗号が付けられた媒体以前に流通したもの）、再生装置／読み取り機はDVD埋め込みデータコードが除外された初期の型式であると検出して、限られた回数での再生アクセスを許す。この再生回数を超えると（トランスポンダ使用者ピットデータフィールド内の運転計数器で追跡されている、図1参照）、該当する媒体の購入または‘使用’ライセンスの更新支払いを促す、取引および更新メッセージが表示される。

【0022】この手法により海賊版媒体物が効果的に著作権所有者に引き渡されるので、更に次の行動に結びつけられるし、また正当に取得した所有者に対して彼らの所有物を適合させることができあり、その一方で著作権所有者に対して価値のある人工統計的情報を供給する。先に説明したハードウェア、ファームウェア／ソフトウェア、副システム方法論の組み合わせは、ブランド付内容物の著作権を保護するための”TIRIS暗号副システム”と呼ばれている。

【0023】別の著作権使用に関する大きな問題は、ディスクのディジタルまたはアナログコピーを別の媒体型式の上に行う場合である。もしも使用者が合法的に著作権保護されているかまたは、保護されていないディスクを持っている場合、その人はMPEGデータストリームに完全にアクセスしたいと思うであろう。本発明の別の実施例によれば、このディジタルデータのコピーを防止する最善の方法は、ディジタル記録装置のデータへのアクセスが制限されたISO-1394データバスを使用する構成である。これはISO-1394のためのIEEE仕様の現存部分に記述されている、送り先周辺機器の論理層のメモリ素子レジスタの中に構築出来る。併用して実施できる別のある方法は、完全に復号されたMPEG

ストリームのみをこの1394バス上に出力することであり、これによって好適な”ディジタル容器”の様な巨大な記憶素子または多数の取り外し可能媒体が実際的でないかまたは経済的に見合わないようにする事である。

【0024】図2は図1のシステムブロックの書き換え可能または記録可能（RAM）版を示す。このRAM版の機能は図1と同様である。

【0025】以下に概要を示す本発明は、基本的に大容量、高品質、ディジタル的に圧縮された内容物を格納するためのDVD、次世代コンパクト／光ディスクに関する著作権および信頼性を保証されたアクセス保護に関する。簡潔のために此處での説明はDVD型媒体のみに限定されているが、本発明は更に広範囲に渡り再生装置／装置に関連するその他のパッケージ化された媒体型式を含む。更に、トランスポンダは單一または多重ページピット機能を具備した読み取り専用または読み取り／書き込み機能を、それらのパラメータを实际上定める価格的な制約そして／またはシステム要求に応じて有することができる。

【0026】以上の説明に関して更に以下の項を開示する。

(1) 著作物のみを任意のディジタル媒体システムの中で再生可能または使用可能とすることを保証するための方法であつて：呼掛信号をトランスポンダに送信しつつそれに応答するトランスポンダ応答信号を受信するための無線周波数呼掛け器を、I/Oポートを有する媒体再生装置に統合し；トランスポンダを予め定められた媒体素子に取り付け、此處で前記媒体素子はディジタル媒体内容物ストリームを有し、また前記トランスポンダは暗号解読アルゴリズムを含むトランスポンダ応答信号を、前記呼掛信号を受信したことに対応して送信する、前記トランスポンダを取り付け；トランスポンダ応答信号を受信した前記暗号解読アルゴリズムをプロセッサに提供し；前記プロセッサを前記ディジタル媒体内容物ストリームを処理するように前記暗号解読アルゴリズムに基づいて構築する、以上のステップを含む前記方法。

【0027】(2) 第1項記載の方法に於いて、前記構築手順が：前記暗号解読アルゴリズムを不揮発性メモリの中にダウンロードし、ここで前記不揮発性メモリの出力が前記プロセッサに入力される、以上のステップを含む前記方法。

【0028】(3) 第2項記載の方法に於いて、前記不揮発性メモリがFlash ROMである前記方法。

【0029】(4) 第1項記載の方法に於いて、前記構築手順が：I/Oポートを構築するための情報を提供するステップを含む前記方法。

【0030】(5) 著作物のみを任意のディジタル媒体システムの中で再生可能または使用可能とすることを保証するための方法であつて：呼掛信号をトランスポンダに送信しつつそれに応答するトランスポンダ応答信号

を受信するための無線周波数呼掛け器を、I/Oポートを有する媒体再生装置に統合し；トランスポンダを予め定められた媒体素子に取り付け、此處で前記媒体素子はデジタル媒体内容物ストリームを有し、また前記トランスポンダは暗号解読アルゴリズム用のポインタを含むトランスポンダ応答信号を、前記呼掛け信号を受信したことに応答して送信する、前記トランスポンダを取り付け；トランスポンダ応答信号を受信したまよめ定められた何処かのアドレスに在る暗号解読アルゴリズム用の前記ポインタを前記媒体再生装置に提供し；前記予め定められたアドレスまたは何処かの予め定められた位置の前記暗号解読アルゴリズムを読み取ってそれらをプロセッサに提供し；前記プロセッサを前記デジタル媒体内容物ストリームを処理するかまたは構築されたI/Oポートにアクセスする情報を提供するように前記暗号解読アルゴリズムに基づいて構築する、以上のステップを含む前記方法。

【0031】(6) 第5項記載の方法に於いて、前記構築手順が：媒体素子を再生または使用するためにどの様に構築するかの命令をプロセッサに提供するステップを含む前記方法。

【0032】(7) 第5項記載の方法に於いて、前記構築手順が：前記暗号解読アルゴリズムを不揮発性メモリにダウンロードし、ここで前記不揮発性メモリの出力が前記プロセッサに入力されるステップを含む前記方法。

【0033】(8) 第7項記載の方法に於いて、前記不揮発性メモリがFlash ROMである前記方法。

【0034】(9) 第1項記載の方法に於いて、前記構築手順が：I/Oポートを構築するための情報を提供す

るステップを含む前記方法。

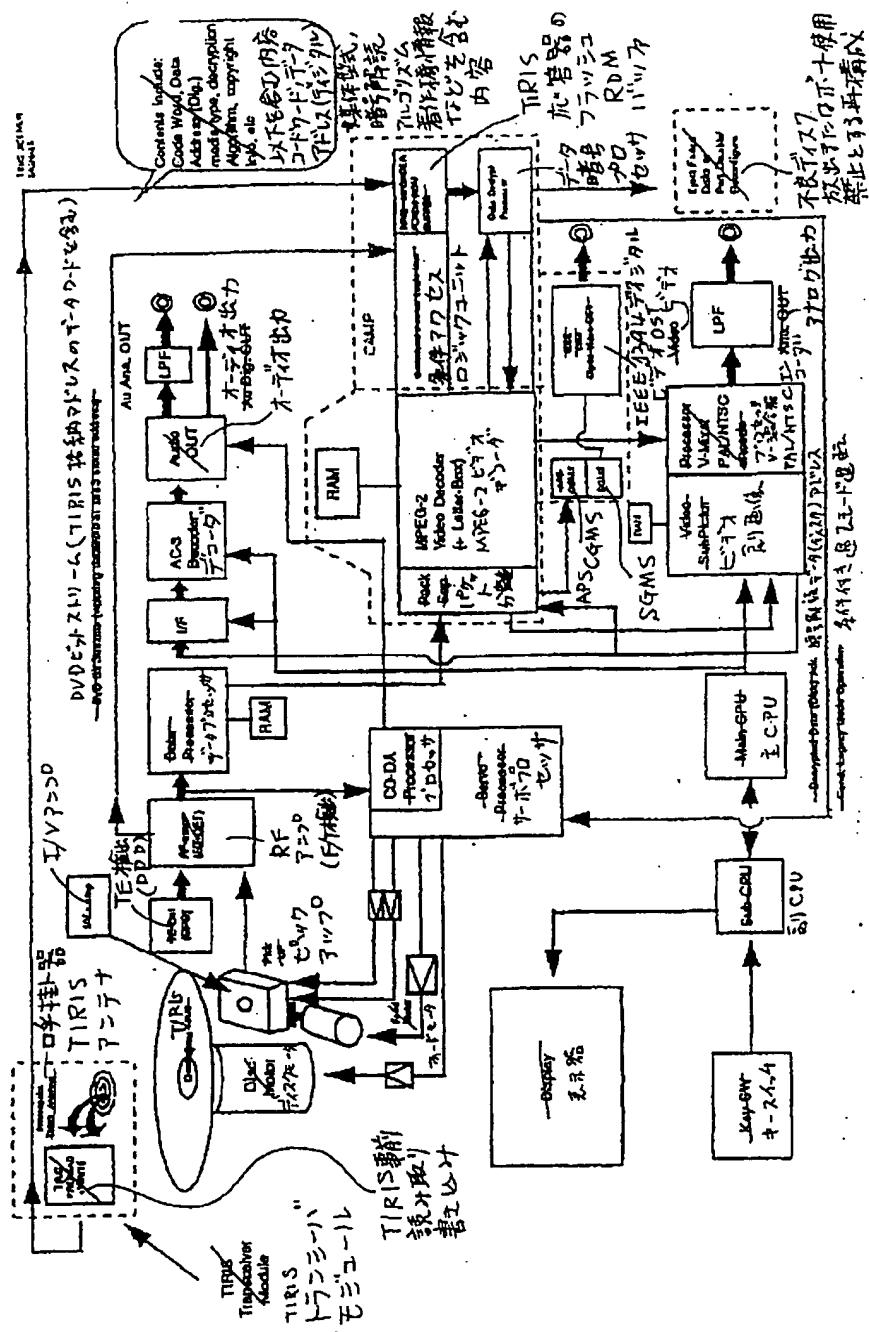
【0035】(10) 本発明は”TIRIS”トランスポンダ（またはその他の無線または赤外線またはバーコードまたはその他の識別装置）を提供されたDVDディスクの中心部に物理的に埋め込むことで構成されている。ディスクが媒体再生装置の中に挿入されると、媒体再生装置の呼掛け器部が呼掛け信号をそのディスク上に配置されているトランスポンダに送信する。この呼掛け信号で充電されると、トランスポンダは予め定められたアドレス、コードワード、暗号化アルゴリズム、媒体型式情報、および著作権情報にそのメモリからアクセスする。次にトランスポンダはそのアドレス、そのコードワード、暗号化アルゴリズム、媒体型式情報および著作権情報を、媒体再生装置内に配置されている呼掛け器に送信し、その呼掛け器はトランスポンダデータストリームを条件付きアクセス管理プロセッサ(CAMP)に送る。CAMPの処理動作と同時に、呼掛け器は再生装置に対してディスク上の予め定められたアドレスに有するデータ_ワードにアクセスするように指令を送り、この再生装置はそのディスク上のデータ_ワードにアクセスする。この媒体再生装置はそのデータ_ワードと受信したコードワードとが一致し、受信したアルゴリズムが媒体の内容を復号する前に正しく暗号解読された場合にのみ再生する。

【図面の簡単な説明】

【図1】図1はDVD再生装置（発表媒体向けROM型式）とTIRIS暗号のブロック図を示す。

【図2】図2はDVD-RAMドライブ（書き込み可能光式）とTIRIS暗号のブロック図を示す。

【図1】



[図2]

